AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A backup/recovery system for protecting a computer system, said backup/recovery system being installed in said computer system, said computer system including an application layer, said application layer being coupled to an interface and operating predetermined application programs, said backup/recovery system BEING CHARACTERIZED BY

- a detecting module, located within said computer system, for monitoring a predetermined data;
- a creating module, located within said computer system, for creating a restore point;

wherein said detecting module retrieves said predetermined data , in order to determine whether there is ~~a predetermined harmful data~~ an executable file contained therein for judging said backup/recovery system to backup data in said computer system or not, said creating module creates a restore point prior to downloading said predetermined data, which contains said executable file, said interface implements a predetermined procedure thereafter and said application layer involves accessing said predetermined data and said backup/recovery system enables restoring said computer system to a previous state which is prior to said downloaded predetermined data arrival.

2. (Previously Presented) The system of claim 1 wherein said backup/recovery system is coupled to a network device, said network device is coupled to at least one client device by a communication link.

3. (Original) The system of claim 2 wherein said network device is coupled to a server device.

4. (Previously Presented) The system of claim 3 wherein said server device is capable of controlling said client device's backup/recovery operation remotely and immediately.

5. (Original) The system of claim 2 wherein said network device comprises a network means, comprising one or more of the group consisting of a LAN, WAN, Internet, Intranet, Extranet and wireless network.

6. (Original) The system of claim 2 wherein said network device comprises a communication means, comprising one or more of the group consisting of electronic mail, TCP/IP sockets, RPC, HTTP, and IIOP.

7. (Currently Amended) The system of claim 1 wherein said ~~predetermined harmful data~~ executable file comprises a file which is of a type that can contain viruses, such as .EXE, .DOC, and .ZIP extension file.

8. (Currently Amended) A method for protecting a computer system, said method comprising:

- Retrieving a predetermined data to be downloaded to said computer system;
- Determining whether there being a predetermined harmful data contained in said predetermined data; ~~and;~~
- Backing up data stored in said computer system at the time said predetermined harmful data being contained in said predetermined data; ~~.~~
- Creating a restore point; and
- Downloading said predetermined data.

9. (Previously Presented) The method of claim 8 wherein said backup/recovery system is coupled to a network device, said network device is coupled to at least one client device by a communication link.

10. (Original) The method of claim 9 wherein said network device is coupled to a server device.

11. (Previously Presented) The method of claim 10 wherein said server device is capable of controlling said client device's backup/recovery operation remotely and immediately.

12. (Original) The method of claim 9 wherein said network device comprises a network means, comprising one or more of the group consisting of a LAN, WAN, Internet, Intranet, Extranet and wireless network.

13. (Original) The method of claim 9 wherein said network device comprises a communication means, comprising one or more of the group consisting of electronic mail, TCP/IP sockets, RPC, HTTP, and IIOP.

14. (Previously Presented) The method of claim 8 wherein said predetermined harmful data comprises a file which is of a type that can contain viruses, such as .EXE, .DOC, and .ZIP extension file.

15. (Currently Amended) A method for protecting a computer system with a backup/recovery system, said computer system including an application layer, said application layer coupled to

an interface and operating predetermined application programs, said method comprising:

- Installing said backup/recovery system in said computer system, said backup/recovery system having a detecting module for monitoring a predetermined data arrived to said computer system;
- Retrieving said predetermined data to be downloaded to said computer system;
- Determining whether there being a predetermined harmful data contained in said predetermined data;
- Backing up data stored in said computer system at the time said predetermined harmful data being contained in said predetermined data;
- Creating a restore point;
- Implementing a predetermined procedure by said interface; and
- Indicating said application layer access said predetermined message.

16. (Previously Presented) The method of claim 15 wherein said backup/recovery system is coupled to a network device, said network device is coupled to at least one client device by a communication link.

17. (Original) The method of claim 16 wherein said network device is coupled to a server device.

18. (Previously Presented) The method of claim 17 wherein said server device is capable of controlling said client device's backup/recovery operation remotely and immediately.

19. (Original) The method of claim 16 wherein said network device comprises a network means, comprising one or more of the group consisting of a LAN, WAN, Internet, Intranet, Extranet and wireless network.

20. (Original) The method of claim 16 wherein said network device comprises a communication means, comprising one or more of the group consisting of electronic mail, TCP/IP sockets, RPC, HTTP, and IIOP.